

Michaud Pushes VA to Fix Data Security

Thursday, May 25 2006

WASHINGTON, DC - Today, Congressman Mike Michaud joined his colleagues on the House Veterans' Affairs Committee in conducting the first of likely many oversight hearings on the recent theft of sensitive information belonging to as many as 26.5 million veterans and spouses from a VA employee's home.

WASHINGTON, DC - Today, Congressman Mike Michaud joined his colleagues on the House Veterans' Affairs Committee in conducting the first of likely many oversight hearings on the recent theft of sensitive information belonging to as many as 26.5 million veterans and spouses from a VA employee's home.

"We need to know how this dangerous breach happened so that we can hold individuals accountable, but more importantly we need to know - right now - what we can do to prevent it from ever happening again and make those changes immediately," said Congressman Michaud. "And we need to take immediate steps to protect the potentially millions of veterans who have been put at risk by this situation."

Congressman Michaud, who serves as the Ranking Member of the Veterans' Affairs Health Subcommittee, pressed the Administration for more details on the internal breaches of secure veteran data and the VA Inspector General's findings on VA's cyber-security and internal control programs. The Committee also received testimony from the Department of Veterans Affairs and organizations on the issue of information security and identity theft.

"While it may be tempting for VA leaders and others to put the blame for this debacle at the feet of one employee, doing so misses the larger problems with VA's IT security," said Michaud. "These larger problems rest not with a single data analyst but the leadership of the VA and its security policies."

The Government Accountability Office has shown that since 1998, the VA has encountered numerous, consistent, and persistent problems with managing its IT programs. VA Inspector General George Opfer testified before the committee about VA data security issues and his office's concern that not enough has been done to secure the personal information of veterans.

"By not controlling and monitoring employee access, not restricting users to only need-to-know data, and not timely terminating accounts upon employee departure, VA has not prevented potential risk," said Opfer. "These weaknesses placed sensitive

information, including financial data and sensitive veteran medical and benefit information, at risk, possibly without detection of inadvertent or deliberate misuse, fraudulent use, improper disclosure, or destruction."

According to the Inspector General, VA has implemented some security enhancements for specific VA locations, but it has not made security corrections VA-wide.

"We believe centralization is essential because standardization is the key to fixing VA information security weaknesses," said Opfer. "As long as three stove-piped administrations and other smaller component organizations are free to operate in the IT environment on their own within VA...the vulnerabilities cannot be effectively resolved."

While VA is taking steps to inform the veterans whose private information was compromised, those potentially affected should visit www.firstgov.gov or call 1-800-FED INFO (333-4636) if they have concerns or questions.

"If we don't tackle the larger issues, then it is only a matter of time before another breach of personal information happens," said Michaud. "We need to focus on the vulnerabilities of VA's data systems rather than focusing on just one individual act. The VA has been a leader in creating a culture of patient safety. The VA needs to learn from this experience and be a leader in creating a culture for data security."

In the long-term, Members of the Veterans' Affairs Committee intend to continue their push for greater VA-wide information security enhancements. In order to specifically address the recent data breach, Michaud and his colleagues are cosponsoring the "Veterans Identity Protection Act of 2006." This legislation would require the VA to provide one year of free credit monitoring to affected individuals. The bill would also provide one free credit report each year for two years after the end of credit monitoring, in addition to the free credit report available under the Fair Credit Reporting Act.

###